

Department of Public Safety

Information Technology Plan

For 2014-2016 Biennium

By

Robert S. Brinson

Chief Information Officer,

Department of Public Safety

Prepared: October 1, 2014

Contents

1	INTRODUCTION	3
1.1	PURPOSE.....	3
1.2	ROADMAP.....	3
2	DEPARTMENT OF PUBLIC SAFETY IT PLAN EXECUTIVE SUMMARY	5
3	GUIDANCE.....	6
3.1	SCIO GUIDANCE	6
4	DEPARTMENT OF PUBLIC SAFETY VISION, MISSION, VALUES AND GOALS.....	8
4.1	VISION.....	8
4.2	MISSION	8
4.3	VALUES.....	8
4.4	AGENCY GOALS.....	8
5	DEPARTMENT OF PUBLIC SAFETY IT VISION, MISSION, AND VALUES.....	9
5.1	IT VISION	9
5.2	IT MISSION.....	9
5.3	IT VALUES	9
6	DEPARTMENT OF PUBLIC SAFETY IT GOALS, OBJECTIVES AND INITIATIVES.....	10
6.1	GOAL 1	10
6.1.1	Objective 1.....	10
6.1.1.1	Initiative 1.....	10
7	DEPARTMENT OF PUBLIC SAFETY IT ORGANIZATIONAL STRUCTURE (REPORTING STRUCTURE).....	11
8	ADDITIONAL AGENCY REQUIREMENTS	12
8.1	INNOVATIVE FUNDING SOLUTIONS.....	12
8.2	OPPORTUNITIES FOR STATEWIDE INITIATIVES	12

1 INTRODUCTION

1.1 PURPOSE

The purpose of this document is to provide agency data for the Information Technology Plan for the 2014-2016 Biennium to the North Carolina State Chief Information Officer (SCIO) as required by G.S. 147-33.72B. The statute mandates that each agency submit a technology plan to the SCIO by October 1 of each even-numbered year. The State Information Technology Plan (Plan) is required to cover a five-year time period. To properly inform the Plan, agency plans are also required to cover a five-year time period.

1.2 ROADMAP

Goal	Objective	Initiative	Description	Funding Mechanism
Goal 1 Deliver a united infrastructure	Objective 1.1 Directory Services	Initiative 1.1.1	Complete AD project	General Fund
		Initiative 1.1.2	ADFS Implementation	General Fund
	Objective 1.2 Data Center consolidation	Initiative 1.2.1	JFHQ project	General Fund
	Objective 1.3 Network rationalization, simplification, cost reduction	Initiative 1.3.1	De-duplication of circuits	N/A
		Initiative 1.3.2	Evaluate WAN architecture	General Fund
	Objective 1.4 Telephony Infrastructure	Initiative 1.4.1	VOIP Project	General Fund

Goal	Objective	Initiative	Description	Funding Mechanism
Goal 2 Use our data for analytics and intelligence	Objective 2.1 Develop improved analytics capability	Initiative 2.1.1	Provide tools for data analysis	TBD
Goal 3 Application rationalization and modernization	Objective 3.1 Understand what applications we have	Initiative 3.1.3	Inventory existing systems	General Fund
	Objective 3.2 Existing Projects	Initiative 3.2.1	Electronic Health Records for inmates (HERO)	General Fund
		Initiative 3.2.2	NCJOIN Juvenile case management improvement	General Fund
		Initiative 3.2.3	JFHQ Data Center consolidation	General Fund
		Initiative 3.2.4	VIPER	General Fund
		Initiative 3.2.5	Victim Notification (SAVAN) contract rebid	Federal grant
		Initiative 3.2.6	School safety	TBD
		Initiative 3.2.7	SAFIS Fingerprint system refresh	General Fund
	Objective 3.3 Planned Projects	Initiative 3.3.1	SBI/ALE case management approach	TBD

2 DEPARTMENT OF PUBLIC SAFETY IT PLAN EXECUTIVE SUMMARY

The Governor and Legislature have vested a lot of confidence in the Department of Public Safety. In 2012, they consolidated three agencies to form the Department. In 2013, they added the Geodetic Survey to Emergency Management. In 2014, they added the SBI, the ABC Commission, and Private Protective Services. Change is something we know a lot about.

Against that backdrop, we have outlined three goals.

The first goal is basic: **delivering a united infrastructure**. Each of the groups noted above come to the department with operational systems in place. Now they need to work with new colleagues in organizational units that have changed. Email, phone systems, shared files and other technology needs to be modified to support their basic daily tasks. This plan describes the actions we are taking to enable the combined workforce to operate well together. However, there are also opportunities. Since each organization came with a working infrastructure, we ought to be able to eliminate duplication. One example is where we share facilities and now have an opportunity to reduce multiple data circuits.

The second goal is to use our assembled data for **improving analytics and intelligence**. While crime rates and prison population are seeing improvements, gang activity and terrorism concerns seem to be increasing. Between the offender information we hold from Adult Correction, the gang information we house for law enforcement across the state, the case information held by ALE and the SBI, the crime incident data we accumulate from local law enforcement, our working partnership with Administrative Office of the Courts to match against their data, and our tight connection with CJLEADS; we have a rich data trove. We can make officers and the public safer with tools like link analysis and predictive analysis.

With the third goal, we look at **coordinating our portfolio of applications**. As we combine the different agencies into one unified DPS, we need to understand what are the key applications, where they are in the life cycle, whether or not we have similar applications that duplicate each other, and where we might bring automation to outdated or manual processes.

3 GUIDANCE

3.1 SCIO GUIDANCE

IT Vision

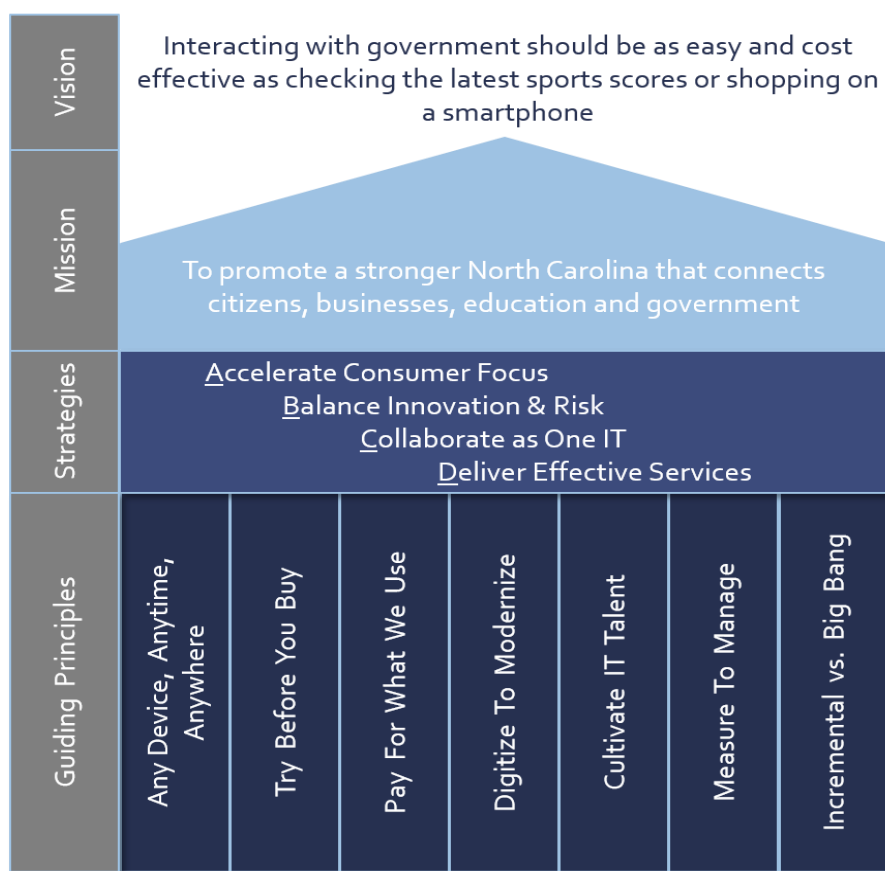
Making government services more accessible and efficient for all consumers is the foundation of the One IT strategy.

IT Mission

Promoting a stronger North Carolina that connects citizens, businesses, education, and government is the mission of IT.

IT Strategies

Strategies focus organizations to achieve complicated goals or objectives. With an eye to the future while sustaining current foundational requirements, the SCIO has adopted the “ABC” strategy to fix and modernize IT.



IT Vision, Mission, and Strategies

Strategy	Intended to:
A. Accelerate Consumer Focus	Embrace the consumerization of IT with a focus on the requirements of the consumer of technology
B. Balance Innovation and Risk	Try newer technologies while managing enterprise risk
C. Collaborate as One IT	Work as a team to accomplish our mission
D. Deliver Effective Operations	Focus on achieving business outcomes through effective and efficient technology delivery

In addition to the seven guiding principles outlined above, the SCIO’s [Cabinet Unite IT Strategy](#) focuses strongly on collaborative IT governance, big data and analytics (to include, but not limited to, work with GDAC and GIS), IT operations, and innovation.

The table below outlines the six IT business capabilities and five IT organizational capabilities highlighted in the Cabinet Unite IT Strategy.

Business Capabilities	Organizational Capabilities
Digital Focus	Collaborative IT Governance
Big Data and Analytics	Strategic Planning and Architecture
Enterprise Resource Planning	IT Program and Project Management
Application and Service Modernization	Innovation
Risk Management and Security	Talent Development and Management
IT Operations	

Please consider these areas, along with the seven guiding principles and your agency-specific goals and objectives when creating agency IT goals and objectives.

4 DEPARTMENT OF PUBLIC SAFETY VISION, MISSION, VALUES AND GOALS

4.1 VISION

The department's motto, "Prevent, Protect, Prepare" describes the vision for public safety in North Carolina.

4.2 MISSION

The overall mission of the Department of Public Safety is to improve the quality of life for North Carolinians by reducing crime and enhancing public safety.

4.3 VALUES

Our law enforcement, correction, National Guard and emergency management capabilities strive to keep North Carolinians safe in their homes, their workplaces and on our roads. In times of natural disaster, emergency management can leverage the resources of the entire department to help North Carolinians recover.

4.4 AGENCY GOALS

The department focuses citizen and legislative attention on law enforcement and public safety issues, such as the supervision of offenders in prison or in juvenile detention centers and in community supervision, drinking and driving, underage access to alcohol and tobacco, the proper use of child safety seats, crime prevention and preparation for natural disasters.

In addition to natural disasters, the department is constantly updating plans and providing training for local officials to respond to emergencies such as terrorism, communicable diseases, nuclear power plant incidents and civil unrest.

This agency serves as the coordinating agency for North Carolina's homeland security preparedness.

In the most recent legislative session, the department has also assumed responsibility for the State Bureau of Investigation, the Private Protective Services Board, and the Alcoholic Beverage Control Commission.

5 DEPARTMENT OF PUBLIC SAFETY IT VISION, MISSION, AND VALUES

5.1 IT VISION

We're the technical staff for a large and diverse department. We try to supply an underlying infrastructure that makes daily work straightforward and seamless. We try to make sure they have what they need before they know they need it. We try to translate complex technical tools and approaches into plain language so our business users understand what we are recommending to them and why it makes sense for their operations.

5.2 IT MISSION

The department performs a range of function critical to all North Carolinians. It operates 24 hours a day every day of the year. The operational mission of the IT staff is to keep the technology systems running on that same basis, with industrial strength backup and disaster recovery. Beyond meeting operational requirements, the IT staff provides leadership in matching new technologies to emerging business needs, and establishing a technical infrastructure that will grow with the department.

5.3 IT VALUES

The IT staff mirrors the high standards of the department's operational units. That means we expect IT staff members to have high ethical standards, meet background check requirements, preserve the confidential nature of data they may encounter in their work, and be prepared to do their jobs in dangerous conditions where their neighbors are well-advised to remain safe at home.

6 DEPARTMENT OF PUBLIC SAFETY IT GOALS, OBJECTIVES AND INITIATIVES

6.1 GOAL 1:

6.1.1 Objective 1:

6.1.1.1 Initiative 1

See attached Section 6 document appended to end of this document. A better formatter than I needs to make it fit in here. Thanks.

7 DEPARTMENT OF PUBLIC SAFETY IT ORGANIZATIONAL STRUCTURE (REPORTING STRUCTURE)

The department's central IT organization reports to the Chief Operating Officer of the agency. In addition to the central IT organization, several significant IT groups exist elsewhere in the department. These include:

- State Highway Patrol technical staff is responsible for much of the core network infrastructure for the Patrol, as well as the CJIN mobile data network and the VIPER voice radio network used by the Patrol and local law enforcement.
- Emergency Management technical staff, who are responsible for some operational aspects of the Joint Force Headquarters data center as it relates to emergency events. Additionally, this group has a particular competency in geographic information systems and data, particularly related to flood plain mapping and flood water prediction. Several years ago, the Geodetic Survey group was moved from another agency into Emergency Management. Data from this group is, among other uses, critical to farmers statewide.
- Adult Correction, which has computer support technicians at a number of the larger prisons. These employees have a dual role of general technical maintenance and computer support. Their computer work is largely assigned out of the department's central helpdesk ticketing system, by agreement with Adult Correction.

Other IT resources exist in smaller numbers around the agency. For the most part, these are power users, application helpdesk staff, business analysts, and other specialized technical skills.

IT resources from the recent State Bureau of Investigation accession are slated to become part of the central IT staff of the department. These resources support a number of critical systems used by law enforcement statewide, both applications and infrastructure.

8 ADDITIONAL AGENCY REQUIREMENTS

8.1 INNOVATIVE FUNDING SOLUTIONS

As a rule, public safety is funded by appropriations, with some additional forfeiture funds, grant funds, and some licensing and permit funds. When we think about innovative funding, receipts come to mind, and significant receipts-based funding is not something that has been in our repertoire. Our core mission is to protect citizens without direct additional charges for those services.

However, one idea may be worth mentioning. The department has a significant GIS capability and so we are part of the state GIS community, which has recently been asked a similar question about monetizing GIS data. We generally think that kind of data, and first-order derivative products of that data, ought to be freely available to citizens and business of the state. But I do think there may be opportunities for value-added services, personalized to a subscriber. The example I'll give stems from any number of mobile phone apps that use location services and tell you when you are near sites of interest, or inexpensive gas, or stores that are having a sale. I think there might be interest in location-based subscription services around a residence using data DPS knows. The value-add would be bringing all the relevant data together. So I might subscribe my residence address, and the service would tell me things like sex offenders moving into or out of the neighborhood, crime incidents and types of crime, localized wind, rain and predictive flood data at my location...all data DPS has. Other agencies have other data of interest that could add to the pool. I might be willing to pay a subscription fee for that kind of service.

8.2 OPPORTUNITIES FOR STATEWIDE INITIATIVES

- Our applications development staff is increasingly being asked to do small applications to address unmet needs in the personnel and financial management areas. For a long time, we forestalled these efforts so as not to duplicate what we hoped BEACON and other enterprise systems would become. However, we can't in good conscience hold them at bay anymore; the business needs are real and urgent. So we have addressed things like: performance rating tracking, fixed asset annual inventory tools, applicant tracking, RIF management, maintenance management, and employee public information release reports. Other agencies' IT staffs are being asked to meet similar needs. We have skilled staff and have done these efforts inexpensively and well, to the delight of our business users. But this is not our core competency as a Public Safety agency, and these needs should be addressed at the enterprise level. (*repeated from prior plan*)
- As a state, I think there is work to be done in the procurement area to focus on time-to-market and sourcing management. We have commented on the PPM process in the past, and that really has not improved. It particularly imperils our agility in the procurement phase of a project. It's easy to ask questions about "how will this work" or "can you assure that this function will operate in this way" but hard to answer them when the answer is dependent on what vendor is selected. There is also now a requirement that any contract over a certain dollar amount get multiple

legal reviews; as a large agency, we are always over that dollar about, even for low-risk, repetitive equipment installations. The result is that we can manage the schedule assiduously up to the gate, and then again once the contract is awarded, but we completely lose control of the schedule for an indeterminate period in between. *(repeated from prior plan)*

- We wonder if it's not time for a fresh look at identity management. As Active Directory has become the standard way of doing business, it seems that it encompasses some of the functions performed by NCID. The answer may still be that NCID adds enough extra value to exceed its cost, but among the agency CIO's, I think there is some doubt. We also have an increasing number of discussions around front-ending our most critical systems with NCID and whether or not the security it adds is worth the extra failure point it brings.

Appendix A: List of Major IT Projects

This purpose of this section is to provide list of major IT projects and applications (>\$250,000) that are in progress or planned in this biennium. The table below maps each project to overall goals and strategies.

Project Name	Short Description	Related Goals and Objectives	Summary of Anticipated Benefits	Approximate Timeframe
Electronic Health Records for Inmates	Moves health records for inmates from paper to digital	6.3	Improves accuracy and portability of inmate records. Assures entries are complete. Gives the ability to search records. Provides better documentation in the event of litigation.	June 2016
NC JOIN Improvements	Updates the juvenile case management tool.	6.3	Improves operational stability. Eliminates a proprietary tool used in the original implementation that has not kept pace with current technology and is now causing problems with system reliability.	March 2016
JFHQ Data Center Consolidation	Moves key department infrastructure to new JFHQ data center	6.1.2	Reduces operational and security risks of running critical department server and storage infrastructure in a number of makeshift server rooms and small data centers. Creates efficient operation through consolidation and virtualization.	December 2014
VIPER	Implements the next phase of the VIPER network and the P25 standard	6.1	Continues the build-out of the Highway Patrol's VIPER voice radio network used by law enforcement statewide, and implements the P25 compatibility standard to ensure interoperability with different radio manufacturers.	October 2014
SAVAN rebid	Seeks competition for the	6.3	This system lets crime victims register to know when an	December

Project Name	Short Description	Related Goals and Objectives	Summary of Anticipated Benefits	Approximate Timeframe
	SAVAN victim notification system		offender is released from custody. The contract with a third-party provider has been in place for a number of years. The number of potential service providers has increased. It's time to rebid.	2015
Enhance analytics and intelligence capability	See section 6.2 description of business problem	6.2	Greater officer safety and improved ability to solve crimes.	Anticipated project; schedule to be determined
SAFIS refresh	Refresh the state automated fingerprint system	6.3	Newer technology that will capture prints better, including the ability to identify from a single print and the ability to capture palm prints.	Anticipated project; schedule to be determined
Common case tool for combined SBI and ALE	Conform the tools the SBI and ALE use to investigate and monitor	6.3	Better unified operation of the two law enforcement groups which will operate as one under DPS.	Anticipated project; schedule to be determined

End of document

The text below is the information for Section 6. It needs to be inserted there and formatted:

6.1 Goal 1: Deliver a united infrastructure

In 2012, DPS was formed from Correction, Crime Control and Juvenile justice. Each agency had infrastructure components such as directory services, email, data centers, etc. In some cases, individual agencies had multiples. In 2014, we added the SBI, Private Protective Services Board, and the ABC Commission. Again, each of those organizations had their own infrastructure approach. This first goal is that we owe the business a unified infrastructure that helps this complex agency operate as a single entity.

6.1.1 Objective 1: Directory services

Making directory services work well is a key to unifying our staff. This becomes more complicated because of the law enforcement security requirements and the requirement that Emergency Management needs to be able to operate autonomously in a disaster. In the current environment, that means we need to operate at least two directories: one for law enforcement and emergency management, and a second for the rest of the agency. We use ITS for that second instance. In spite of having two directories, we need to operate across the agency on a trusted basis, sending emails, scheduling meetings and conference rooms, and sharing network drives among workgroup members.

6.1.1.1 Initiative 1: Complete the Active Directory project

We are finishing a project to move Adult Correction from Novell to Enterprise Active Directory (EADS). All other department components are already on AD, and will be sorted into either EADS or the Law Enforcement AD.

6.1.1.2 Initiative 2: ADFS implementation

As we wrap up the project above, then we are starting a final step to use federation (ADFS) and any other appropriate tools to bridge the gap between the multiple directories. Since the bulk of the department is on EADS, this will require the cooperation of ITS.

6.1.2 Objective 2: Data center consolidation

One of the initial projects as the agency came together was a consolidation of the various server rooms and makeshift data centers around the state. Since we had the new Joint Force Headquarters (JFHQ) with data center in place, we elected to use that as our primary data center, and

the WDC as our backup. With the accession of the SBI, we now have to review our options, since they have a well-thought-out data center on the Garner campus, and an agreement with MCNC for a backup facility, both meeting CJIS security requirements.

6.1.2.1 Initiative 1: JFHQ project

We are in production at the JFHQ now, and have a schedule to move our most critical systems. We have begun to virtualize our servers to a much greater degree than we were able to before. As a result, we are beginning to decommission server rooms.

6.1.3 Objective 3: Network rationalization, simplification, cost reduction

The department has physical facilities all over North Carolina. As we combine, we realize we are paying for multiple circuits to facilities we share or which are very close to another facility. While we have looked at this during the first two-and-a-half years of consolidation and made some improvements, with the addition of the SBI, we think there are new opportunities to reduce costs or to hold costs constant while upgrading to higher bandwidth options.

6.1.3.1 Initiative 1: De-duplication of circuits

6.1.3.2 Initiative 2: Evaluate WAN architecture

Much like the special pricing available for education, there are similar opportunities for law enforcement. As an example, MCNC has, as a part of their mission, support of public safety. We intend to look at circuit cost and availability options that might reduce costs. We also want to look at more high-bandwidth backhaul options that might mesh with the regional office consolidation that is part of the department's overall strategy.

6.1.4 Objective 4: Telephony infrastructure

The department has adopted the Cisco VOIP solution that was being used by Crime Control as a standard approach. We are working now to move into the constant traffic flow of offices upgrading their existing phone systems or requiring a new phone system as they move from one leased facility to another. This unified communication approach is important to overall connectivity across the agency, but it also fits our business model of a mobile work force and the ability to have phone calls follow the worker, regardless of where they are.

6.1.4.1 Initiative 1: VOIP project

The build-out of central Raleigh administrative offices is nearing completion. Additionally, prior to the SBI consolidation, we had mutually agreed to pool contractual resources and infrastructure on the Garner Campus as a cost-saving approach. This has proved to be an excellent decision, because they now come to DPS with the same telephony architecture as we have.

6.2 Goal 2: Capitalize on rich data sources for analytics and intelligence

One of the purposes for adding the SBI to the department is to assemble criminal justice operations and data in a single place. The department recognizes an opportunity to use this data to protect the public and to keep our employees and local law enforcement safe as they perform their duties.

6.2.1 Objective 1: Develop improved analytics capability to apply against multiple large criminal justice datasets.

As examples, we already have a good tool (CJLEADS) to paint a complete picture of an offender. But we also have data about gangs, crime incidents, money transfers to and from inmates, inmate phone calls, inmate visitors (who they are, who they visited, when they visited, etc.) that exist outside CJLEADS. Linked together, this data can associate individuals and give law enforcement a better starting point to solve crimes.

6.2.1.1 Initiative 1: Provide tools for data analysis

We will work with GDAC to determine the best way to approach this opportunity. At a high level, we see these activities:

- Assess the data sources we now hold
- Define our starting business requirements and objectives. At the outset, we are interested in bringing to law enforcement a complete picture of an individual, tailored to the role of the officer and the situation.
- We will work with CJLEADS to see how that tool works to solve this problem.
- Evaluate specialized tools for link analysis and predictive analytics
- Determine how this activity fits with the Fusion Center

6.3 Goal 3: Application rationalization and modernization

6.3.1 Objective 1: Understand what applications we have.

As the CIO's have mutually agreed, the Application Portfolio Management (APM) tool has not proved to be the useful working repository of application information that we all hoped it would be; new approaches are in the works. Until then, we need to assemble a listing of our applications that is useful for our purposes.

6.3.1.1 Initiative 1: Inventory existing systems.

List the systems. Understand what they do. Look at life cycle, cost of maintaining, staff and tool set which supports them. Look for duplications.

6.3.2 Objective 2: Existing projects

A number of significant projects are already underway. The ones listed below are significant by virtue of critically, cost, time, staff resources, or key administration initiatives.

6.3.2.1 Initiative 1: Electronic Health Records for Inmates (HERO)

This will move our adult inmate population from a paper health record to an electronic record. Female facilities are done. Male facilities will begin to move in the next few months. This sets us up for better record keeping, more uniform treatment, better defense in the event of litigation, and easier record transfer, both from prison to prison, and eventually, we hope, to community services for released inmates.

6.3.2.2 Initiative 2: NC JOIN

This is a rework of part of our juvenile case management system. Proprietary software was used as one component of the original build. That technology is no longer supported and is causing stability issues. Because of the proprietary nature, our visibility into issues is extremely limited, making resolution difficult. The project will remove the proprietary software to improve stability and diagnostics.

6.3.2.3 Initiative 3: JFHQ Data Center Consolidation

As previously discussed, this leverages the new data center in the Joint Forces Headquarters building, slowing eliminating multiple substandard local server rooms and small data centers, which moving us to increased virtualization.

6.3.2.4 Initiative 4: VIPER

While not classically an application, VIPER is a critical statewide infrastructure system operated by the State Highway Patrol. VIPER projects continue the build-out of the statewide system of towers and transmitters, and also move the system to the P25 open standard.

6.3.2.5 Initiative 5: Victim notification (SAVAN) contract rebid

We contract for a notification service to crime victims. Victims, court officials, law enforcement officers and others can register to be notified if an offender is about to be released from a prison or from any jail in the state. The existing vendor has held the contract for a number of years and new competitors have entered the market. It is time to rebid the service, and will necessitate changes in how data is passed from Adult Correction and the 96 jails to the vendor.

6.3.2.6 Initiative 6: School safety

The Center for Safer Schools is housed in the department. They are in the process of finding a service provider to supply a mobile app for students to report tips or alert authorities about incidents at their school. Elsewhere in the department Emergency Management is contracting for a mobile app that will help first responders in responding to school incidents. The app will map the school building, the roads, the nearby hospitals, where the utility shut-off are, etc.

6.3.2.7 Initiative 7: SAFIS fingerprint system refresh

The SBI's system of automated fingerprint identification is due for refresh in the next 2-3 years. This is a significant capital outlay that is critical to the state's criminal justice community. The new system will take advantage of technology improvements that have occurred since the last refresh.

6.3.3 Objective 3: Planned projects

6.3.3.1 Initiative 1: SBI/ALE case management approach

As the SBI and ALE come together into a single law enforcement group, each has a case management tool. We will evaluate the functionality of both tools, look at the combined business requirements, and decide on an approach for a single system of managing cases.

